IDAHO ITS

# Building a Foundation for Responsible AI

Office of Information Technology Services

## Why This Work Matters

*AI is here — Idaho is getting ahead of it*

- AI tools are being adopted across state government at a rapid pace
- Without clear rules, agencies risk using AI in ways that could harm citizens or expose the state to legal and security risk
- ITS responded with two major deliverables this year:

**Idaho's AI Advantage Framework**

*Statewide governance for responsible AI adoption*

**Guide to Data & Systems Classification**

*Defining how sensitive data must be handled before AI can touch it*

# Idaho's AI Advantage Framework — 8 Core Principles

*Grounded in ethical rigor and practical implementation — with people at the center*

**01**
**Human-Centered Design**
Technology serves people

**02**
**Transparency & Explainability**
Know when AI is involved

**03**
**Appropriate Oversight**
Humans stay in charge

**04**
**Fairness & Accessibility**
Works equally for all Idahoans

**05**
**Security & Privacy by Design**
Data protected from the start

**06**
**Risk-Based Governance**
Higher stakes = stricter review

**07**
**Continuous Improvement**
Systems monitored over time

**08**
**Shared Responsibility**
ITS sets rules; agencies implement



# Guide to Data & Systems Classification

*Before AI can be used on state data, we must know: how sensitive is that data?*

| | |
|---|---|
| **Level 1** **Unrestricted / Public** | Public agency information created for general consumption |
| **Level 2** **Limited / Internal** | Sensitive internal data — examples: audit reports, emails |
| **Level 3** **Restricted / Confidential** | Federally regulated, agency-use only — example: medical records |
| **Level 4** **Critical** | Disclosure could cause significant harm, injury, or loss of life |

**M365 Copilot GCC approved for Levels 1–3** · Classification must be determined before any AI tool is used on the data

## Microsoft 365 Copilot GCC — Now Available to All State Agencies

*A secure AI assistant built into the tools you already use every day*

**What It Does**

- Summarizes emails, meetings & documents
- Drafts responses using your actual work context
- Analyzes data in Excel — no formulas needed
- Turns Word documents into PowerPoint decks
- Works in Word, Excel, PowerPoint, Outlook & Teams

**Why the GCC Version Matters**

- Built specifically for government use
- Data never leaves the state's secure environment
- U.S.-only data centers — no offshore processing
- Does NOT train on your data
- Approved for Level 1, 2 & 3 data

Free Copilot Chat available now to all employees · Paid M365 Copilot license requestable via ITS Service Portal



# AI Agents & MCP: The Next Chapter

*Where ITS is heading — pilots underway now*

# From Assistant to Agent — What's the Difference?

*Copilot answers your questions. Agents get things done.*

| AI Assistant — What We Have Now | AI Agent — Where We're Going |
|---|---|
| You ask, it answers | **You set a goal — it figures out the steps** |
| One task at a time | **Handles multi-step workflows automatically** |
| You stay in the loop for every action | **Checks in only when human judgment is needed** |
| Like a knowledgeable colleague | **Like a capable staff member who can act** |

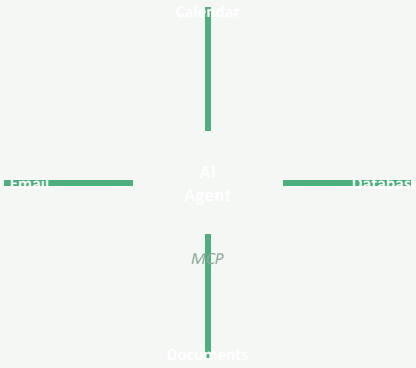
*Think of it like: asking how to file a claim vs. handing it to someone and saying please file this for me — agents do the second thing.*



# What is MCP? — The Universal Connector for AI Agents

*Model Context Protocol — the plug that lets AI securely connect to your systems*

- MCP stands for Model Context Protocol
- Think of it as a universal power strip — instead of custom-wiring every system, MCP gives AI a single standardized connection
- Without MCP: every agency system integration must be custom-built from scratch — slow and expensive
- With MCP: agents securely connect to databases, calendars, documents, and case files in one controlled way
- ITS controls what each agent can access and what actions it is allowed to take
- Permissions stay in place — agents only see what they are authorized to see



# AWS AgentCore — The Platform Powering Idaho's Agents

*Enterprise-grade, secure infrastructure for building and running AI agents at scale*

| | |
|---|---|
| **Runtime** | Each agent runs in its own isolated environment — one agent can never access another's data |
| **Gateway + MCP** | Connects existing agency systems to AI agents using MCP — no need to rebuild current systems |
| **Identity** | Manages secure access — agents only get credentials for what they are authorized to use |
| **Memory** | Agents remember context from past interactions to serve citizens more effectively over time |
| **Observability** | ITS can audit every step an agent takes — full visibility into what it did and why |
| **Policy Controls** | Plain-language boundaries set by ITS — agents are automatically stopped if they violate the rules |

*ITS is adopting the AgentCore work pioneered by Boise State University — standing on proven ground rather than starting from scratch.*



# Our Partner: Boise State University

*ITS is building on what Boise State has already proven — not starting from scratch*

| 30,000 Students | 1,400 Faculty | 3-Person Team | 6 Months to Launch | 80%+ Cost Reduction |
|---|---|---|---|---|

### What Boise State Built

- Built boisestate.ai — a campus-wide secure AI platform on AWS
- Data privacy first — does not train AI models on institutional data
- Agents & MCP already on their roadmap — automate tasks and connect AI to campus systems like Canvas, calendars, and library databases
- Demonstrates what is possible for Idaho state government at scale

### What ITS Is Doing With It

- ITS is adopting and extending their AWS AgentCore implementation
- Active pilots underway now — leveraging their proven architecture
- Shared mission: responsible AI that serves the public without compromising privacy
- A model for state-university collaboration on emerging technology

# What AI Agents Could Look Like for Idaho Agencies

*Real possibilities — built on the AgentCore and MCP foundation we are piloting now*

### Benefits Processing

- Receives application
- Checks eligibility criteria
- Routes to correct reviewer
- Days of work done in minutes

### Scheduling & Routing

- Citizen requests appointment
- Agent checks availability
- Books slot & sends confirmation
- Zero staff involvement needed

### Document & Data Retrieval

- Staff ask a plain English question
- Agent searches across systems
- Surfaces the right answer instantly
- No manual digging required

### Meeting Follow-Up

- Agent joins the meeting
- Summarizes key decisions
- Drafts action items
- Updates the right case files automatically



# Every Agent Idaho Builds Follows the Same Rules

*Safety and accountability are built into the foundation — not added as an afterthought*

### Risk Assessment Required

- Every agent goes through ITS's formal risk assessment before deployment
- High-risk use cases receive rigorous review before going live

### Human Oversight Stays In Place

- Agents assist — they do not replace accountability
- Humans remain responsible for all high-stakes decisions

### MCP Gives ITS Precise Control

- ITS defines exactly what each agent can and cannot access
- Access can be revoked or adjusted at any time

### Full Auditability

- AgentCore logs every step an agent takes
- ITS can review exactly what was done and why

## The Next Frontier: AI That Lives on Your Device — Ollama

*Exploring local AI — private, offline, and free to run*

**Data Never Leaves the Device**

- AI runs entirely on local hardware
- Nothing sent to any external server
- Ideal for Level 3 & Level 4 sensitive data

**Works Without Internet**

- Field staff and rural offices stay productive
- No dependency on cloud availability
- Always on — no outages or downtime

**Eliminates Per-Use Cloud Costs**

- Free and open source — no license fees
- No per-use charges at scale
- Download once, run unlimited times

*ITS is currently in the research and exploration phase — evaluating hardware requirements, model performance, and security implications before any broader rollout.*

Idaho Office of Information Technology Services its.idaho.gov/ai

# Questions?

**Idaho Office of Information Technology Services · its.idaho.gov/ai · 208-605-4000**